

Commission nationale de l'informatique et des libertés

Délibération n° 2014-239 du 12 juin 2014 portant autorisation unique de mise en œuvre, par les professionnels et établissements de santé ainsi que par les professionnels du secteur médico-social habilités par une loi, de traitements de données à caractère personnel ayant pour finalité l'échange par voie électronique de données de santé à travers un système de messagerie sécurisée

NOR : CNIX1416668X

La Commission nationale de l'informatique et des libertés,

Vu la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique, notamment ses articles L. 1110-4, L. 1111-8, L. 6316-1 et R. 6316-1 à R. 6316-11 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 8-IV et 25-II ;

Vu la loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013, notamment son article 48 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu l'arrêté du 6 février 2009, modifié en dernier lieu par l'arrêté du 2 octobre 2013, portant création d'un traitement de données à caractère personnel dénommé « Répertoire partagé des professionnels de santé » (RPPS) ;

Vu l'arrêté du 12 juillet 2012 relatif à la mise en place d'un traitement de données à caractère personnel dénommé ADELI de gestion de l'enregistrement et des listes départementales de certaines professions et usages de titres professionnels ;

Après avoir entendu M. Alexandre LINDEN, commissaire, en son rapport et M. Jean-Alexandre SILVY, commissaire du Gouvernement, en ses observations,

Décide :

La présente autorisation unique concerne les traitements de données à caractère personnel ayant pour objet de permettre l'échange de données de santé au moyen d'un service de messagerie sécurisée de santé entre professionnels de santé et, plus largement, entre les professionnels des secteurs sanitaire, social et médico-social habilités par une loi à collecter et à échanger des données de santé à caractère personnel.

Ces échanges doivent être réalisés dans des conditions de sécurité respectueuses des dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée et de celles du code de la santé publique, notamment ses articles L. 1110-4 et L. 1111-8. En outre, tout service de messagerie sécurisée de santé doit également respecter les référentiels de sécurité et d'interopérabilité mentionnés aux articles précités.

Les utilisateurs finaux des services de messagerie sécurisée de santé sont les professionnels de santé et les professionnels habilités par une loi à collecter et échanger des données de santé à caractère personnel dans le cadre de leurs missions (ci-après dénommés « professionnels habilités »). Une telle habilitation est prévue par l'article 48-IV de la loi n° 2012-1404 du 17 décembre 2012 de financement de la sécurité sociale pour 2013.

La présente autorisation concerne les responsables de traitement qui recourent à un système de messagerie sécurisée de santé, que celui-ci soit développé par le responsable de traitement ou par un opérateur tiers auquel il a recours.

L'utilisation de messageries sécurisées de santé aux fins d'échanges de données de santé à caractère personnel, dans le cadre du suivi ou de la prise en charge de patients, poursuit un intérêt public et relève dès lors des dispositions des articles 8-IV et 25-I de la loi du 6 janvier 1978 modifiée.

Dans ce contexte, la commission décide, en application de l'article 25-II de la loi du 6 janvier 1978 modifiée, que les responsables de traitement de messagerie sécurisée de santé qui lui adressent une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Tout traitement de données à caractère personnel qui excéderait le cadre ou les exigences définis par la présente autorisation unique doit, en revanche, faire l'objet d'une demande d'autorisation spécifique.

Art. 1^{er}. – Sur les finalités du traitement.

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente autorisation unique les traitements de données à caractère personnel mis en œuvre ayant pour finalité de permettre des échanges de données de santé au moyen d'un service de messagerie sécurisée de santé entre « professionnels habilités ».

Les professionnels habilités ou les structures au sein desquelles ils exercent sont identifiés par les référentiels nationaux d'identification des personnes physiques et des personnes morales des secteurs sanitaire, social et médico-social suivants :

- le répertoire partagé des professionnels de santé (RPPS) ;
- le répertoire ADELI (automatisation des listes) ;
- le répertoire FINESS (fichier d'identification nationale des établissements sanitaires et sociaux) ;
- le répertoire SIRENE (système informatique pour le répertoire des entreprises et de leurs établissements).

Ces professionnels peuvent également être identifiés par un référentiel d'identification local, c'est-à-dire propre à la structure dans laquelle le service de messagerie sécurisée de santé est déployé.

Le référencement d'une personne physique ou morale au sein d'un référentiel d'identification est réalisé à l'issue d'un processus de vérification de l'identité et de la fonction de la personne.

La qualité de responsable de traitement est attachée soit au professionnel lui-même lorsqu'il exerce en libéral, soit à la structure sanitaire, médico-sociale ou sociale au sein de laquelle il exerce, en fonction des statuts et des missions de ladite structure.

Les actes de télémedecine opérés au moyen d'une messagerie sécurisée de santé doivent être réalisés conformément aux dispositions du code de la santé publique, notamment ses articles L. 6316-1 et R. 6316-1 à R. 6316-11.

Art. 2. – Sur la nature des données traitées.

Les seules données à caractère personnel pouvant être traitées sont les données relatives aux professionnels habilités, celles des patients qu'ils prennent en charge et à propos desquels des échanges d'informations sont nécessaires pour assurer la qualité et la sécurité de cette prise en charge, ainsi que les données relatives aux personnes en charge de l'administration de la messagerie.

1° Données relatives aux professionnels utilisateurs finaux dits professionnels habilités :

S'agissant des professionnels habilités, peuvent être traitées les catégories de données suivantes :

- les données d'identification (état civil), l'identifiant du professionnel (numéro d'enregistrement au répertoire partagé des professionnels de santé [RPPS], numéro d'enregistrement au répertoire ADELI ou numéro d'identification local) et les données relatives au moyen d'authentification ;
- les coordonnées professionnelles (adresse, numéros de téléphone, adresse de courriel) ;
- le(s) titre(s) professionnel(s) ;
- les adresses de messagerie sécurisées de santé créées ;
- les données techniques nécessaires à la fourniture du service de messagerie sécurisée de santé (adresse IP, cookies) ;
- les traces des actions opérées sur la messagerie sécurisée de santé ;

2° Données relatives aux personnes concernées par les données échangées :

S'agissant des personnes concernées par les données échangées entre professionnels habilités, peuvent être traitées les catégories de données suivantes :

- les données d'identification (nom, prénom, date et lieu de naissance, sexe), éventuellement l'identifiant national de santé ;
- les coordonnées (adresse, numéros de téléphone, adresses de courriel) ;
- les informations strictement nécessaires à la prise en charge des personnes et relatives à leur état de santé, à leur situation sociale ou à leur autonomie ;

3° Données relatives aux personnes en charge de l'administration des équipements et logiciels mis en œuvre pour la messagerie sécurisée :

S'agissant des personnes en charge de l'administration des équipements et logiciels mis en œuvre pour la messagerie sécurisée, les données strictement nécessaires à leur identification peuvent être traitées (identifiant de la personne physique, nom, prénom, fonction) afin de tracer leurs actions sur le système.

Art. 3. – Sur la durée de conservation des données.

Le service de messagerie sécurisée ne se substitue en aucun cas au dossier médical, sanitaire ou médico-social de la personne concernée (le patient) que doivent tenir les professionnels habilités susvisés en vertu des obligations légales et réglementaires qui leur incombent. Il constitue uniquement un outil professionnel d'échange sécurisé de données de santé, et non un nouvel espace de stockage.

Sans préjudice de dispositions législatives ou réglementaires propres à certaines catégories de données imposant une durée de conservation particulière ou la suppression des données visées à l'article 2, les responsables de traitement employant des personnes habilités doivent veiller à ce que ces données ne soient pas conservées au-delà de la période d'activité de ces professionnels.

Les professionnels de santé ayant la qualité de responsable de traitement doivent veiller à respecter la même obligation s'agissant des données qu'ils traitent.

Afin d'être conforme à la présente autorisation, un service de messagerie doit comporter un système permettant d'organiser la suppression des boîtes aux lettres (BAL) en cas d'inactivité complète, caractérisée par l'absence d'authentification de l'utilisateur pendant une période maximale d'un an.

Toute suppression doit être systématiquement précédée d'une information de l'utilisateur par le canal de son choix, afin de lui permettre, le cas échéant, de s'opposer à cette suppression.

Les modalités et le rythme d'envoi de ce message d'alerte sont portés par tout moyen à la connaissance de l'utilisateur, par exemple dans les conditions générales d'utilisation du service de messagerie sécurisée.

Durée de conservation des traces techniques :

Les traces techniques sont les traces des actions enregistrées automatiquement par le système (système d'exploitation, équipements réseaux et de sécurité : pare-feu par exemple) et par les composants applicatifs. Elles englobent les traces de connexion et de déconnexion au système de messagerie sécurisée de santé (authentification de l'utilisateur ou de la machine) ainsi que les traces des actions réalisées par les opérateurs techniques du système.

Les traces techniques sont conservées pendant un an.

A l'issue des durées de conservation susmentionnées, les données sont définitivement supprimées.

Art. 4. – Sur les destinataires des données.

Les destinataires des données sont les destinataires des messages échangés au moyen de leurs messageries sécurisées de santé, ayant la qualité de « professionnels habilités » telle que définie en préambule de la présente autorisation unique.

La commission rappelle que les professionnels de santé et les professionnels habilités sont soumis au secret professionnel prévu à l'article 226-13 du code pénal.

Les personnes en charge de l'administration de la messagerie peuvent accéder aux données relatives aux professionnels utilisateurs finaux dans le strict cadre de leurs missions et dans le respect du secret des correspondances privées. Elles doivent, en outre, être soumises à une clause de confidentialité.

Art. 5. – Sur l'information des personnes.

Sur l'information des patients :

Il appartient au responsable de traitement d'informer clairement les patients de la finalité du service de messagerie sécurisée de santé, de ses conditions de mise en œuvre, y compris en cas d'hébergement des données auprès d'un hébergeur agréé à cet effet, ainsi que des modalités d'exercice de leurs droits.

Ces modalités doivent être portées à la connaissance des patients par la remise d'une brochure d'information, ou à défaut par voie d'affichage ou par une mention dans les livrets d'accueil des structures les prenant en charge.

Sur l'information des professionnels habilités :

Le responsable de traitement doit informer les professionnels habilités des conditions d'utilisation du service de messagerie sécurisée de santé et des modalités d'exercice de leurs droits.

Cette information doit notamment porter sur le respect des dispositions en matière de confidentialité figurant à l'article L. 1110-4 du code de la santé publique relatives aux conditions d'échange de données de santé entre deux ou plusieurs professionnels de santé.

La commission recommande que chaque professionnel soit informé qu'il lui appartient de veiller à ce que toute information qu'il jugera utile pour la prise en charge de ses patients soit reportée dans leur dossier médical.

Le responsable de traitement doit informer les professionnels habilités que les traces de leurs actions peuvent être conservées.

Une communication électronique émise ou reçue par une personne peut revêtir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles 226-15 et 432-9 du code pénal. Le responsable de traitement informe les professionnels habilités des modalités permettant de différencier les courriels professionnels des courriels personnels qu'ils peuvent être amenés à échanger par le biais du système de messagerie sécurisée. Toutefois, la commission rappelle que les données relatives à la santé des personnes doivent être traitées dans des conditions de confidentialité conformes à l'article L. 1110-4 précité. Dès lors, elles ne doivent être accessibles qu'aux professionnels habilités intervenant dans le cadre de la prise en charge des personnes.

La commission rappelle que ces informations doivent être formalisées dans un document, tel qu'une charte informatique, qui doit être porté à la connaissance des personnes concernées.

Art. 6. – Sur les droits d'accès, de rectification et d'opposition des personnes.

L'exercice des droits d'accès, de rectification et d'opposition des personnes concernées par les données traitées (professionnels habilités, patients) s'opère auprès du responsable du traitement de messagerie sécurisée de santé.

En cas d'opposition du patient à l'échange de données le concernant au moyen d'un service de messagerie sécurisée de santé, les professionnels habilités doivent cesser tout échange le concernant par le biais de cette messagerie et recourir à un moyen d'échange alternatif (courrier postal par exemple).

Art. 7. – Sur la sécurité des données.

Le responsable de traitement prend toutes précautions utiles pour préserver la sécurité des données traitées, afin notamment d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

A cet effet, le responsable de traitement doit utiliser un service de messagerie sécurisée de santé conforme aux exigences de sécurité imposées par l'article 34 de la loi du 6 janvier 1978 modifiée.

Il doit réaliser ou s'assurer qu'a été réalisée, lorsqu'il fait appel à un prestataire éditeur d'une solution de messagerie sécurisée de santé, une analyse des risques que le système de messagerie fait peser sur les libertés et la vie privée des personnes concernées.

Conformément aux dispositions du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, le responsable de traitement est tenu, le cas échéant, d'attester de sa conformité aux exigences du référentiel général de sécurité (RGS) et de rendre cette attestation accessible au public.

Les services de messageries sécurisées de santé doivent assurer une identification et une authentification fiables des professionnels habilités, afin de garantir la confiance dans ces dispositifs.

La mise en place d'un service de messagerie sécurisée de santé doit, en outre, satisfaire aux conditions suivantes :

1. Le service de messagerie doit garantir l'identité de l'émetteur et du destinataire d'un message en vérifiant leur appartenance à un référentiel d'identification national ou local.

Le responsable de traitement est garant de l'identification et de l'authentification des professionnels habilités.

La commission rappelle qu'en application de l'article 6-1° de la loi du 6 janvier 1978 modifiée un traitement de données à caractère personnel doit satisfaire à une condition de licéité. Dès lors, pour la création d'un compte de messagerie, le responsable de traitement est tenu de s'assurer de l'identité de l'utilisateur final et de son exercice légal de la profession. Lorsque des comptes de messageries dits « organisationnels ou applicatifs » sont créés, ceux-ci n'identifient pas une personne physique, mais un service, un secrétariat, un automate ou toute forme d'organisation. Cette création est réalisée sous la responsabilité du responsable de traitement de la structure auquel ils se rattachent. En tout état de cause, le responsable de traitement doit veiller à ce que les traces d'accès à ces comptes de messagerie permettent d'identifier la personne physique qui a accédé au compte applicatif ou organisationnel.

Pour l'accès et l'utilisation d'un compte de messagerie :

- s'agissant des professionnels de santé, l'authentification doit être réalisée au moyen d'une carte de professionnel de santé (CPS) ou d'un dispositif équivalent agréé par l'organisme chargé d'émettre la CPS ;
- s'agissant des autres professionnels habilités, l'utilisateur final doit s'authentifier de manière forte, c'est-à-dire par un procédé qui requiert au minimum deux facteurs d'authentification distincts parmi ce que l'on sait (par exemple un mot de passe), ce que l'on a (par exemple un certificat électronique ou une carte à puce) et une caractéristique qui nous est propre (par exemple une empreinte).

Le service de messagerie sécurisée de santé doit être doté d'un dispositif assurant la traçabilité des actions d'utilisation et d'exploitation du service. Ces traces doivent être conservées dans des conditions permettant d'assurer la sécurité des données, notamment leur pérennité et leur intégrité.

2. Le service de messagerie doit assurer la sécurité des messages et des pièces jointes lors de leur transfert.

Le service de messagerie sécurisée de santé doit être mis en œuvre de façon à garantir la sécurité des messages et pièces jointes, notamment leur confidentialité et leur intégrité durant leur transfert entre le poste des professionnels habilités (l'utilisateur final-émetteur et l'utilisateur final-destinataire).

A cette fin, le recours à des moyens de chiffrement conformes à l'état de l'art pour protéger le transfert des messages et des pièces jointes est obligatoire.

3. Le service de messagerie sécurisée de santé doit assurer la conservation sous une forme sécurisée des messages et des pièces jointes.

Lorsque le responsable de traitement développe lui-même le service de messagerie sécurisée de santé utilisé par les professionnels habilités et qu'il conserve par ses propres moyens les serveurs de messagerie sécurisée de santé, il est tenu de mettre en place les moyens techniques et organisationnels adéquats.

Le responsable de traitement doit ainsi assurer la disponibilité, l'intégrité, la traçabilité et la sécurité physique et logique des messages et des pièces jointes qu'il conserve.

Les moyens mis en œuvre doivent être conformes à l'état de l'art et adaptés à la finalité d'un service de messagerie sécurisée de santé. Ces moyens doivent correspondre aux mesures de sécurité retenues au terme d'une analyse des risques.

Lorsque le responsable de traitement ne conserve pas par ses propres moyens les données de santé à caractère personnel échangées et collectées par le biais d'un service de messagerie sécurisée de santé, il doit veiller à ce que les serveurs de messagerie soient conservés par un hébergeur agréé à cet effet, dans les conditions conformes aux articles L. 1111-8 et R. 1111-9 et suivants du code de la santé publique.

L'hébergeur ainsi agréé garantit la disponibilité, l'intégrité, la confidentialité et la traçabilité des données de santé.

Lorsque le responsable de traitement utilise un service de messagerie sécurisée de santé développé et fourni par un prestataire, il doit s'assurer que celui-ci respecte l'ensemble des dispositions du présent article 7.

Art. 8. – Publication.

La présente délibération sera publiée au *Journal officiel* de la République française.

La présidente,
I. FALQUE-PIERROTIN